# Midnight Blizzard hack: How ITDR could have saved Microsoft

**Identity-based attacks are on the rise, but they can be prevented with the right identity threat detection and response measures.**

As winter crept in last year, so did a threat actor. Microsoft revealed in January that the Russia-backed group Midnight Blizzard (aka Nobelium) had compromised senior-level email accounts and stolen sensitive information in a password-spraying attack dating back to November 2023.

Thought to be affiliated with the Russian Foreign Intelligence Service, Midnight Blizzard performs espionage attacks on targets across the US and Europe. The group is perhaps best known for the SolarWinds hack in 2020 – a massive supply chain breach that affected thousands of organizations, including the US government.

Midnight Blizzard's latest attack on Microsoft was sophisticated but easily preventable. A protective layer of identity threat detection and response (ITDR) measures would have stopped the group from gaining a foothold in Microsoft's corporate environment. In this blog, we'll look at how.

## How it happened

In late November 2023, Midnight Blizzard used a password-spraying attack to compromise an old Microsoft test account that didn't have multifactor authentication (MFA) enabled. To avoid being detected or locked out of the system, the group used residential proxy networks to masquerade as legitimate users and focused its attack on a small number of accounts.

With a foothold in the system, Midnight Blizzard took over a legacy test OAuth application connected to Microsoft's corporate environment and created more OAuth applications. It leveraged the privileges that came with these to grant itself the Office 365 Exchange Online *full_access_as_app* role, which provided access to the entire 365 stack. In what Microsoft says was a bid to find information about itself, Midnight Blizzard then stole data such as documents and emails from senior-level accounts.

"The Microsoft security team detected a nation-state attack on our corporate systems on January 12, 2024", Microsoft disclosed in an 8-K filing, "and immediately activated our response process to investigate, disrupt malicious activity, mitigate the attack, and deny the threat actor further access."

The breach, which Microsoft detected in log data when reviewing Exchange Web Services, apparently didn't affect customer environments, production systems, source code, or AI systems, and was solely identity-based – Midnight Blizzard didn't exploit any vulnerabilities in the company's system.

## The attack flow, in brief

- **Initial access:** Password-spraying attack
- **Privilege escalation:** Abuse and duplication of OAuth applications
- **Data exfiltration:** Theft of information from senior-level email accounts
- **Covering tracks:** Use of residential proxy infrastructure and a precise, low-volume password-spraying attack
- **Mitigation:** Detection via Exchange Web Services activity and denial of further access

## On password spraying

This technique is the equivalent of throwing things at the wall and seeing what sticks. Attackers take a set of common passwords, which are often stolen and sold on the dark web, and use them on a large number of accounts. 'Spraying' passwords in this way is heavy-handed, but if just one works, that's all the attackers need – they've gained access.

Legacy accounts and applications are a common attack surface. They often lack the latest security controls, as well as an active user who can monitor failed logon attempts and verify suspicious activity. With no MFA in place, Microsoft's test tenant was particularly susceptible to password spraying. Midnight Blizzard likely knew this – it focused the attack on only a small number of accounts.

## What can we learn from this?

Microsoft is lucky that Midnight Blizzard didn't abuse its access privileges more aggressively within the 365 stack – it certainly had the chance to do so. When business-critical identities are left unsecured across cloud infrastructure, SaaS apps, and identity providers like this, they can give threat actors catastrophic levels of access.

Basic identity protections shouldn't be used as a crutch. It's clear from this incident and the recent uptick in identity-based attacks (including the 2023 Okta breaches) that organizations must equip their identity and access management (IAM) providers with an extra layer of protection – ITDR. At Rezonate, we believe that the right ITDR solution is essential for strengthening weak authentication controls before attackers can exploit them and shut down security threats. Here are some good ITDR practices to consider:

### Set up MFA

Following the attack, Microsoft admitted its mistake: “If the same team were to deploy the legacy tenant today, mandatory Microsoft policy and workflows would ensure [MFA] and our active protections are enabled to comply with current policies and guidance.”

Microsoft’s test tenant was compromised because it didn’t have MFA enabled. The company failed to monitor its identities properly, and this left a gaping hole in its defenses. ITDR solutions can remove this attack surface by ensuring users have strong passwords to begin with, and by integrating with MFA options to lay down a solid identity security base. They also offer stronger, phishing-resistant authenticators for highly sensitive assets.

### Close the barn door

If attackers gain a foothold in IAM infrastructure using a trusted identity, it’s vital to shut them out as quickly as possible to prevent them from escalating their privileges. The key here is to silo your network. ITDR solutions can spot the gaps in your post-authentication controls and help you enforce stricter privileges and trust relations to make it harder for attackers to move freely in your system.

### Think outside the (in)box

Comms channels like email inboxes are stepping stones for attackers to move laterally and escalate their privileges. Though Microsoft hasn’t said what permissions its legacy account had that gave Midnight Blizzard a foothold, we know that they led directly to the heart of its corporate environment. Consider the blast radius of an attack. ITDR solutions can offer a clearer view of where your privileges lead and help you protect them with password policies, lockout procedures, and session lifetime limits for admin roles.

### Always be on the lookout

It’s good practice to constantly monitor unusual activity and draw up an action plan for a potential attack. ITDR solutions offer real-user and entity behavior and analytics tools powered by machine learning that can automatically analyze correlations, track suspicious behavior, generate alerts, and shut down compromised identities in real time.

## Wrap up

Identities are now our most vulnerable asset. And as we’ve seen with Microsoft, attackers only need to find one crack in your identity infrastructure to inflict serious damage. That’s why it’s so important to combine your IAM system with a protective layer of post-authentication measures. The right ITDR solution can provide a smart, orchestrated response to incidents across cloud, SaaS, and identity provider applications to prevent identity-based attacks like the one Microsoft suffered.